



WHITE PAPER

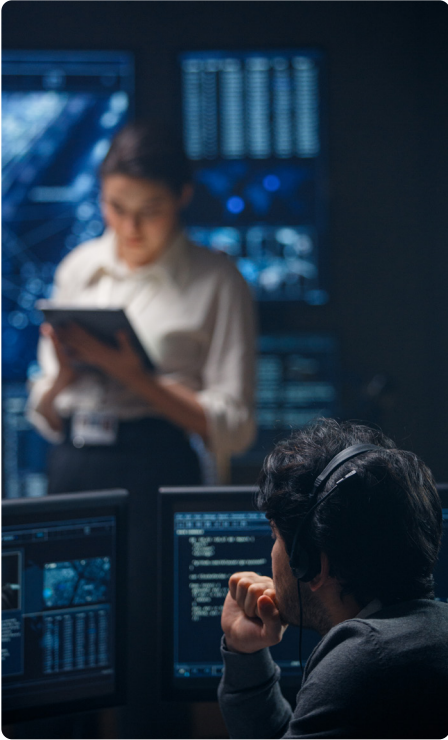
Modernizing authentication across the Federal Government with phishing-resistant MFA

Meet Zero Trust and phishing-resistant MFA requirements and
address emerging use cases



Contents

3	Authentication challenges across federal government
5	The cyberattack landscape adds pressure to modernize defenses
6	New regulations mandate phishing-resistant MFA
9	YubiKey offers FIPS-validated phishing-resistant MFA for federal agencies
12	Common authentication scenarios across the federal government
18	Yubico offers simple procurement and distribution at scale
18	Takeaway



Authentication challenges across federal government

The critical need to address gaps in PIV/CAC authentication

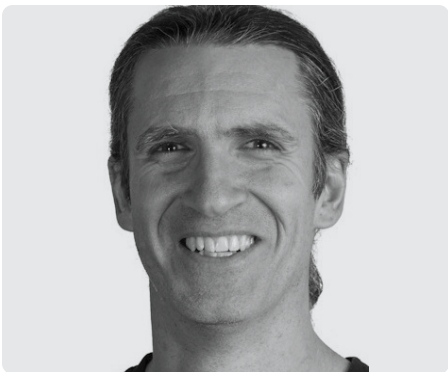
The Federal Government relies on public key infrastructure (PKI) to meet strict information security guidelines. The two tokens in use across the government are the civilian Personal Identity Verification (PIV) and the Common Access Card (CAC), smart card standards in line with Homeland Security Presidential Directive 12 (HSPD 12) and Federal Information Processing Standards (FIPS) 201-3 specifications.

While PIV and CAC meet the needs for traditional perimeter-based and desktop federal authentication requirements, the modernization of IT and related devices and the growth of remote work have created cases where PIV and CAC aren't the most suitable forms of authentication.

From non PIV/CAC eligible employees and contractors to BYOAD (Bring Your Own Approved Devices), cloud services, or air-gapped/isolated networks and even military scenarios where relying on a PIV or CAC may inadvertently reveal identities, there are a growing number of use cases requiring alternate highest assurance multi-factor authentication (MFA). This is particularly important to address the situations where the traditional fallback authentication method has been just a username and password.

The need for highest assurance authentication is not new. In 2016, Terry Halvorsen, then the DoD CIO, noted, "It's really hard to issue a CAC card when people are dropping mortar shells on you and you need to get into your systems."¹ These cases spurred several memos, such as 'Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems' in August 2018, that specifically address the need for DoD-approved MFA when either a system or application does not support authentication using DoD-approved PKI credentials, or a portion of the system or application's subscribers are unable to obtain DoD approved PKI credentials."² The Office of Management and Budget (OMB) issued two memos (M-19-17³ and M-20-19⁴) that laid the groundwork for federal agencies to seek out and adopt other strong authentication as alternatives to the PIV and CAC.

The Defense Information Systems Agency's (DISA) Purebred solution is a government-owned credentialing process for mobile devices, a recognition of growing PKI challenges and the need to modernize CAC. Purebred provides derived credentials to DoD-issued mobile devices and approved external authenticators. While the number of derived credential use cases continues to expand, including the HSPD 12 amendment during COVID-19 to create a Derived Alternate Credential (DAC) to support remote work, the



“ U.S government agencies may be slow to adopt and are still relying on PIV and CAC standards, physical readers, and smart cards, but the pandemic and the move to remote work has raised a sense of urgency in a lot of government agencies. They need better tools that are additive to current tools (PIV/CAC), especially those with more modern architectures and features rather than replacements.”

John Fontana, Program Manager for Standards, Yubico

current derived credential process requires significant investment in systems and in hardware⁵. In a growing number of use cases, users could have multiple derived credentials, one for each government-owned device.

The federal government was already taking active steps to address its identity and authentication challenges when faced with a spike in attacks on critical infrastructure that triggered Executive Order (EO) 14028, “Improving the Nation’s Cybersecurity,” which mandated agencies adopt a Federal Zero Trust Strategy and phishing-resistant MFA as a baseline⁶.

As government agencies look to support the growing number of authentication requirements that do not fit PIV/CAC or that require derived credentials, they are seeking a cost-effective, secure solution for highest assurance authentication in line with Zero Trust principles and with the 2023 National Institute of Standards and Technology (NIST) guidance on PIV credentials outlined in SP 800-157r1 and SP 800-217. Phishing-resistant authentication leveraging the Fast Identity Online (FIDO) standard is well placed to help government agencies extend the benefits of PKI to a wider number of applications, domains and devices—all the areas where traditional PIV and CAC deployments have proven difficult or impossible.



While an employee using PIV is the ultimate security goal, what happens when a PIV is either not available or not compatible with the access requirements? Employees lose PIV cards and it may take days, weeks, or months for an employee to receive their new or replacement PIV. An agency should have a phishing-resistant alternative when a PIV card is not available. Allowing username and password as a backup option should not be the default policy exception.”

—GSA Identity Lifecycle Management Playbook⁷



The cyberattack landscape adds pressure to protect credentials

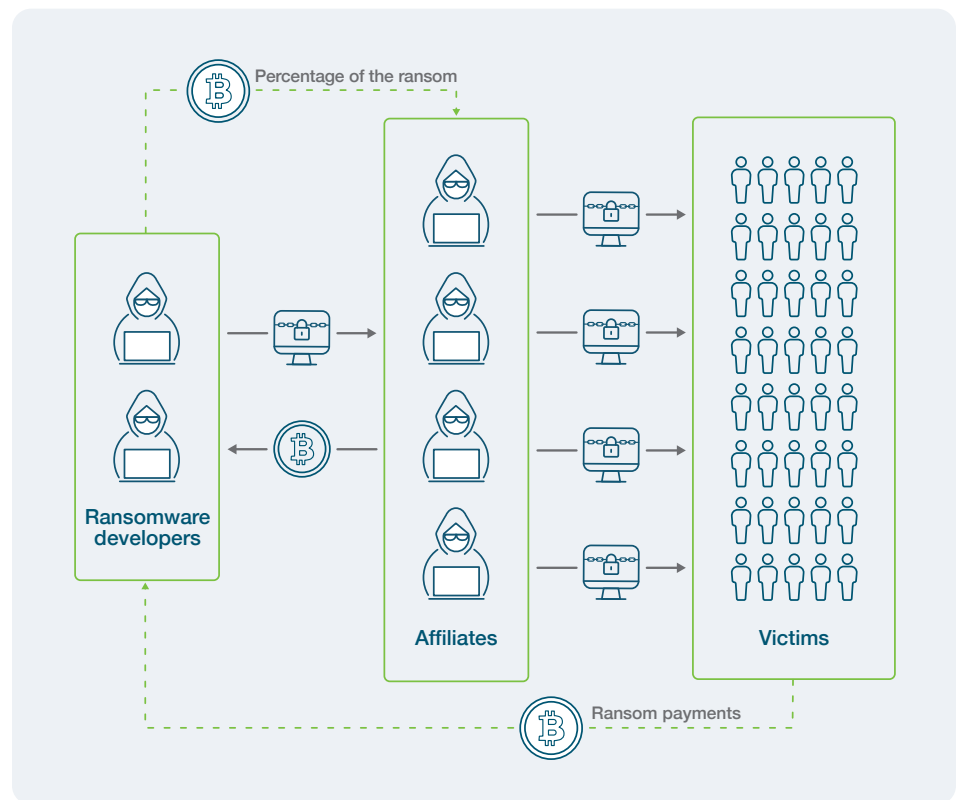
Government entities are under persistent cyberattack from threat actors who leverage sophisticated technologies that often combine different actions including malware, phishing and/or hacking. These complex attacks are often linked with the use of stolen credentials, including notable attacks against the Colonial Pipeline and SolarWinds⁸.

The 2021 Colonial Pipeline attack, an attack that shut down 45% of the fuel for the east coast of the United States and resulted in a \$4.4 million ransom, originated from compromised credentials used to access a legacy virtual private network (VPN) system that lacked MFA⁹. The 2020 SolarWinds attack, one of the worst cyber-espionage incidents on record, traced back to the supply chain and privilege abuse.¹⁰ A 2023 audit of the US Department of the Interior also found that 89% of high value assets were unprotected by MFA and more than one-fifth of active user passwords were easily cracked.¹¹

With almost every breach, you'll find credentials, keys, and secrets abused anywhere they can be. A ransomware attack, for example, most often involves infiltrating an organization through stolen credentials or phishing, which targets credentials. Once inside, the attacker has a path to collect data before “executing” the ransomware attack. The attack goes undetected because the attacker simply logs in disguised as a legitimate user.

“Cybersecurity is a top priority for this administration, and recent events, such as the SolarWinds cyber incident, have shown that adversaries continue to target Federal systems.”

President Biden FY2022 Budget¹²



The evolving attack landscape has triggered increased federal attention on modernizing the nation’s cybersecurity defenses and strengthening supply chain security, with an increased focus on protecting credentials with phishing-resistant MFA.



New regulations mandate phishing-resistant MFA

The Executive Order on improving the Nation's Cybersecurity triggers new requirements

President Biden has made cybersecurity a top priority for Federal agencies, signing EO14028 on improving the nation's cybersecurity on May 12, 2021 outlining key areas that need to be addressed to protect critical digital infrastructure.¹³ The order and subsequent OMB Memo M-22-09 mandate the requirement to adopt phishing-resistant MFA as part of deploying a Zero Trust Architecture.¹⁴ Similarly, National Security Memorandum 9 (NSM-8) reiterated this call to action for defense systems.¹⁵

M-22-09 highlights the critical MFA gap that exists with the many common approaches to MFA that will not protect against sophisticated phishing attacks. Instead, the memo requires agencies to ensure their users are using a phishing-resistant method to access agency-hosted accounts such as providing users with phishing-resistant tokens. To support this memo, NIST has revised its technical requirements for phishing-resistance in NIST SP 800-63-4 to include either channel binding or verifier name binding, processes that rely on cryptographic verification between devices or between the device and a domain.¹⁶

Only two authenticators meet the revised standards as phishing-resistance: the federal government's Personal Identity Verification (PIV) standard and the World Wide Web Consortium (W3C)'s open 'Web Authentication' standard.

“ Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys.”

John Kindervag
Creator of Zero Trust

What qualifies as phishing-resistant MFA?

Phishing-resistant authentication protocols



Channel Binding
PIV/Smart Card



Verifier Name Binding
FIDO2/WebAuthn



While any authenticator assurance level (AAL) will require FIPS 140 validation, NIST SP 800-63-4 clarifies that only AAL3 meets the OMB burden of phishing-resistance, requiring proof of possession of a key through cryptographic authentication protocol capable of resisting phishing attacks. The combination of hardware security key plus FIDO2/WebAuthn meets the requirements of AAL3.

Agencies are required to discontinue support for authentication standards that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications. These new standards must be met by the end of Fiscal Year 2024.

In June 2022, the General Services Administration (GSA) created an M-22-09 Action Plan in the form of an Identity Lifecycle Management Playbook designed to help agencies create an Identity, Credential, and Access Management (ICAM) system agile enough to support modern needs.¹⁷ This playbook recognizes a growing mandate to shift government agencies away from managing the lifecycle of credentials to managing the lifecycle of identities—a shift that recognizes a broad set of use cases that are not well served by PIV/CAC.

Identity-Centric Versus Credential-Centric¹⁸

User authentication can either be deployed at an identity-centric level, or a credential-centric level. Identity-centric authentication mechanisms ensure comprehensive coverage across both legacy and modern applications, allow for fine-grained authorization, and future proof access.

 Identity-Centric	 Credential-Centric
Enable Single Sign-On for agency applications	Manage authentication at each individual application.
Federate application for external partner access.	Application-specific authentication using a PIV card or Username and Password.
Support a variety of phishing-resistant authenticators with a path toward a total passwordless architecture.	Only support PIV card authentication or Username and Password as a backup.
Leverage attributes aggregated through a Master User Record (MUR) for fine-grained authorization.	Leverage attributes only from a PIV Card for authorization.





NIST SP 800-63-4

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 *Digital Identity Guidelines* are currently in public review for a revision that would update all four volumes of the standard¹⁹. The draft SP 800-63-4 guidelines retain the basic organizational structure and assurance level models, but introduce several changes which are designed to reflect the current and emerging attack landscape.

Key changes in the draft guidelines.²⁰

Base Guidelines	800-63A Identity Proofing and Enrollment	800-63B Authentication	800-63C Federation and Assertions
Digital identity model <ul style="list-style-type: none"> Better role definition Separate model for federation 	Guidance for digital identity evidence	Phishing-resistance <ul style="list-style-type: none"> Added requirements for phishing-resistant authenticators per OMB M-22-09 	Redefined FALs <ul style="list-style-type: none"> Stronger verification and protection requirements
Digital identity risk management <ul style="list-style-type: none"> Updated risk management model to address emerging attacks Addition of continuous evaluation 	Guidance for collecting identity attributes <ul style="list-style-type: none"> Identity proofing requires core attribute validation 	Activation secrets <ul style="list-style-type: none"> Guidance for access to stored secret key 	Bound authenticators <ul style="list-style-type: none"> Required for FAL3
	Expanded scope for validation sources	New session management thresholds	Federation agreements
	Privacy risk assessments	Broad range of MFA permitted for AAL2 AAL3 requires proof of possession and phishing-resistance	Provisioning & identity APIs

NIST PIV Credential Updates

In 2022, NIST released a revision to PIV standards ([FIPS 201-3](#)) that allowed federal agencies to verify employee identities and issue credentials remotely, and expand beyond PIV cards to also use FIDO, a standard based on public key cryptography to support authentication to online services.

At the start of 2023, NIST revised its *Guidelines for Derived PIV Credentials* ([SP 800-157r1](#)) and released new *Guidelines for Personal Identity Verification (PIV) Federation* ([SP 800-217](#)). These updates expand the use of derived PIV credentials to new form factors, PKI-based and non PKI-based, and to help support PIV identity outside the home agency. These updates make it possible to support identity credentials for employees and contractors with non-PKI based phishing-resistant authenticators such as a hardware key based upon FIDO2/WebAuthn.

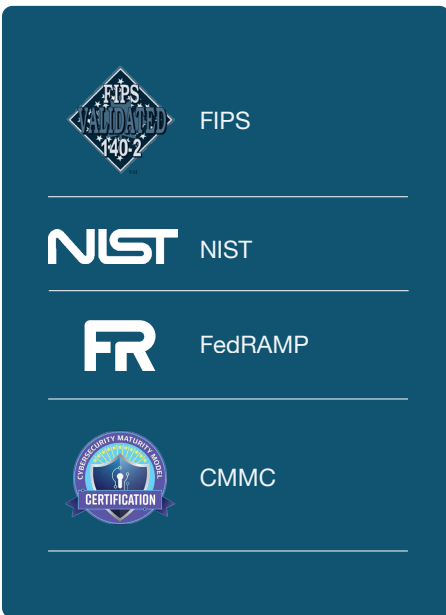


FedRAMP and CMMC 2.0

When adopting cloud services, federal agencies pay careful attention to cybersecurity standards: Federal Risk and Authorization Management Program (FedRAMP) and the DoD's Cybersecurity Maturity Model Certification (CMMC), programs which each saw recent revisions that include requirements for strong MFA to reduce supply chain risks.

FedRAMP is a US government-wide program that provides a standardized approach to evaluate, authorize and continuously monitor cloud service providers (CSPs) and cloud service offerings (CSOs). In response to EO 14028, the Cybersecurity and Infrastructure Security Agency (CISA), the US Digital Service, and FedRAMP released version 2.0 of the Cloud Security Technical Reference Architecture guide with security requirements in line with Zero Trust.²¹

The CMMC program is an audit process that combines various security standards (NIST, ISO, AIA and DFARS) into one standard.²² In 2021, an enhanced CMMC 2.0 program was announced to simplify the CMMC standard and provide greater clarity on requirements, including the requirement for MFA.²³ An estimated 70,000 DoD contractors are required to become **CMMC certified**, with certifications now also being rolled out new RFIs and RFPs.²⁴



YubiKey offers FIPS-validated phishing-resistant MFA for federal agencies

The YubiKey is a DoD-approved²⁵ FIPS 140-2 validated hardware security key that provides highest assurance, phishing-resistant alternate authentication for PIV/CAC. The multi-protocol YubiKey offers the options of both Smartcard (PIV) and FIDO authentication protocols, enabling agencies support for both legacy and modern applications and services on a single key, and a path to modernization while supporting systems in place currently. Additionally, the YubiKey supports derived credentials such as Purebred (PIV) or, looking to the future, from the Defense Manpower Data Center (DMDC). A single security key can be used to securely authenticate users to applications and services across multiple government issued or personal devices such as laptops, desktops, tablets, and mobiles, without the need for additional hardware or software, making it a secure and cost-effective solution.

As a portable hardware root of trust, YubiKeys offer the best available security against phishing attacks and account takeovers and offer a seamless path to meet new Zero Trust and MFA requirements. With the YubiKey as a portable root of trust, users can:

- Rapidly convert any device into a trusted device
- Have a portable credential to authenticate seamlessly across multiple devices
- Experience fast account recovery in case of a lost or stolen device



YubiKeys are available on the Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) as a preferred authenticator to meet OMB Memo M-19-17.

Today



Alternate hardware authenticator to PIV/CAC



Derived PIV/CAC credentials

Tomorrow



Passwordless FIDO2 protocol

Key Features



Multi-Protocol

Support for WebAuthn, FIDO U2F, FIDO2, smart card (PIV), Yubico OTP, OATH-TOTP, OATH-HOTP, and Challenge-Response



Easy to Use

No battery or network connectivity required, users simply insert and tap to authenticate to computers, networks, online applications and services



Government Certified

FIPS 140-2 validated, Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3

DoD Cybersecurity Maturity Model Certification (CMMC) Level III compliant

FedRAMP High



Broad Ecosystem

Deploy instantly with Microsoft Azure AD, Centrify, Duo, Ping, Okta, Google and works across major operating systems including Microsoft Windows, macOS, Android, Linux and major browsers.



AAL 3

Validated to NIST SP 800-63-3 Authenticator Assurance Level (AAL) 3 requirements



Compliant

Compliant with DFARS / NIST SP 800-171 / HSPD 12

DoD Cybersecurity Maturity Model Certification (CMMC) Level III compliant

The YubiKey's hardware design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied or stolen. YubiKeys are manufactured securely in the US using stringent processes and a secure supply chain for trustworthy components.

The YubiKey is designed for both strong security and usability, with no requirement for network connectivity, cellular connection or batteries to work—in addition to being water and crush-resistant. To authenticate, users simply tap or touch their security key. YubiKeys are available on the Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) as a preferred authenticator to meet OMB Memo M-19-17.

YubiKeys are a DoD-approved alternate phishing-resistant authenticator to help meet use cases where PIV/CAC are not available or suitable or to accommodate derived PIV/CAC credentials.



YubiKey for PIV/CAC

HSPD-12 identifies four criteria for secure and reliable forms of identification, including—but not limited to—a PKI-based smart card credential (following FIPS 201²⁶). Alternatively, agencies can use one-time PIN tokens and one-time PIN mobile applications for phishing-resistant non-PKI authenticators, such as FIDO2 supported on the YubiKey.²⁷

The Yubikey is one of only three DoD CIO government approved alternate authenticators that meet DoD's rigorous cybersecurity requirements for non-classified and secret classified environments.

A single YubiKey can be used to securely authenticate users to applications and services across multiple government-issued or personal devices such as laptops, desktops, tablets, and mobile phones. The YubiKey has out-of-the-box native integration for the Microsoft environment using Smart Card/PIV functionality based on NIST SP 800-73.

YubiKey for derived credentials

The YubiKey includes a secure built-in chip that accommodates Purebred derived PIV/CAC requirements for secure credentialing in line with the technical requirements of NIST SP 800-157. As a portable root of trust, the YubiKey can support multiple devices, services or secure offices, reducing hardware costs and solving use cases around BYOAD, cloud services, and even secure offices. To meet the OMB M-22-09 requirement, the YubiKey becomes a strong hardware-based identity token that is tied to a master identity record in Azure AD, which ties into CBA.

While derived credentials stored on a device are a security risk, credentials stored on YubiKeys cannot be extracted or tampered with. As a side benefit, if a mobile or computer device is lost or stolen, or a new device issued, the YubiKey can be used as an easy method to establish or re-establish trust with online accounts and re-register the internal authenticator on a new device.

Just as importantly, the YubiKey looks and acts like a PIV/CAC for both the system and the user, making it a light IT project with minimal end user training requirements.

A future-proof solution

As government agencies adopt newer authentication standards and protocols in the future such as WebAuthn/FIDO2, YubiKeys can easily transition from smart card PIV and CAC credentials to support newer FIDO-based authentication. This makes them the best choice for a portable root of trust today; and tomorrow when government agencies are ready to adopt modern FIDO2 authentication standards.

“ The most common way to integrate non-PKI-derived credentials is through a modern Single Sign-On tool or operating system that supports FIDO2 or WebAuthn.”

GSA Identity Lifecycle Management Playbook²⁸



Common authentication scenarios across the federal government

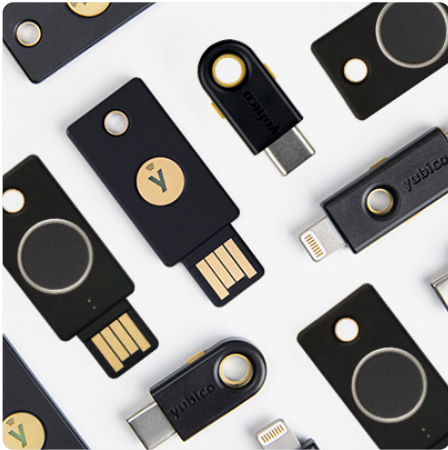
While PIV and CAC remain the primary means of identification for authentication to federal systems, facilities and secured areas, the shift to managing identity supports a more comprehensive set of use cases. With the YubiKey, agencies can deploy highest-assurance, phishing-resistant MFA to support a variety of authentication scenarios across the federal government, including:



Non PIV/CAC eligible employees & contractors

The YubiKey leverages WebAuthn/FIDO2 to help agencies meet phishing-resistant MFA across any and all access points being used by employees, contractors and partners—whether in-person, hybrid or remote. For example, the YubiKey can help support phishing-resistant authentication to government services and systems for short term contract workers, retirees, or other non-PIV/CAC eligible users. Some users may even require a token that works by itself without additional smart card hardware or software needs.

Many commonly used access points such as VPNs, IdPs (Identity Provider), cloud platforms, desktop login, and web access offer support today either for webAuthn, PIV, or both. The chart below shows an example of common access points that support phishing-resistant MFA using either WebAuthn/FIDO2, or PIV, as well as YubiKey support.



Phishing-resistant authentication options

The chart below shows an example of common access points that support phishing-resistant MFA using either WebAuthn/FIDO2, or PIV, as well as YubiKey support. Check with your technology partners to validate their capabilities.

Access points		Offers webAuthn support	Offers PIV support	YubiKey (webAuthn/FIDO and/or PIV)
On premise (active directory)	Windows 10+ Login	✓ /3rd party	✓	✓
	Earlier versions of Windows Login	3rd party	✓	✓
	macOS Login on a Windows domain	3rd party	✓	✓
	VPN Access	Varies	✓	✓
	Secure Proxy Gateways	✓	Varies	✓
Cloud platforms	Microsoft Azure	✓	Preview / Federation	✓
	Amazon Web Services (AWS)	✓	✓ / Federation	✓
	Google Cloud	✓	Federation	✓
	Oracle Cloud	✓	Federation	✓
	IBM Cloud	✓	Federation	✓
IDPs	Okta	✓	✓	✓
	Ping	✓	✓	✓
	DUO	✓	N/A	✓
	ForgeRock	✓	✓	✓



New York Air National Guard leverages the YubiKey for high-assurance network authentication

The New York Air National Guard (NY ANG) often faces situations where personnel have legitimate needs to access DoD networks, but who are not eligible for a PIV credential or CAC. Retired military personnel, reservists, and members of the Army and Air Force National Guards often serve only part-time, losing the ability to leverage a CAC. In some cases, Reserve and Guard members have a CAC, but are not issued government-furnished equipment (GFE), so lack a CAC reader.

To meet the needs of National Guard personnel and others, the Defense Department approved the use of three alternate multi-factor authentication (MFA) solutions when PKI is infeasible - including the YubiKey, a FIPS 140-2 validated alternative to the PIV or CAC that allows non-CAC personnel or personal non-GFE devices in a BYOAD environment to securely authenticate to DoD networks.

The New York Air National Guard began rolling out YubiKey in a test program in 2021 to let senior guard members authenticate to a New York State emergency management system, and progressively to DoD CAC credential-enabled sites with personnel, financial, and healthcare services. The YubiKey was also critical to supporting the 30% of the workforce who want to continue to work remotely.

“This protects the security of the military but also gives you the flexibility to meet the demanding needs of COVID-19 or whatever might come next,” notes Maj. Ali, “I want to be able to fight my battle with smart people from all over the world by getting them network access to help me execute our missions. That is the future vision.”

Aside from supporting the millions of retired members who continue to access medical and financial systems, the YubiKey can also serve as an alternate authenticator to CAC by supporting derived PIV/CAC credentials (DISA Purebred).

“

I think sometimes we only focus on the 650,000 people we have currently in the total force, and forget about the millions of people that are already retired and their family members that need access to secure medical information, paychecks, and digital transactions. With the YubiKey, they would be able to better secure their accounts with strong multi-factor authentication.”

Maj. Liaquat “Rocket” Ali, Remote Piloted Aircraft Cyberspace Officer at the New York Air National Guard

Workstation login

Government workers that use shared devices/workstations can benefit from a portable root of trust similar to the PIV and CAC. They can authenticate to the network using the trusted smart card credential on their YubiKey, proving they are a trusted user.



Cloud-based software/productivity software

For civilian agencies and select DoD groups, YubiKey can authenticate to existing Identity and Access Management (IAM) and SSO solutions (Microsoft, Google, Okta, Duo, Ping) to provide federated access to web applications and service-related apps, providing additional AAL3 capabilities to traditional IdP solutions.

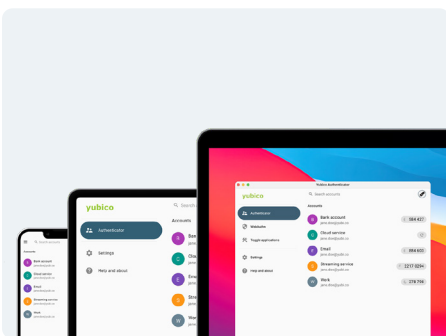
Microsoft users, either Azure, Azure Active Directory (Azure AD), or Microsoft 365, can take advantage of native support for the YubiKey for immediate compliance with the authentication requirements of OMB M-22-09 in a Zero Trust framework. With Azure AD Cloud Native CBA and YubiKeys, agencies can leverage the YubiKey as a PIV card with Active Directory Federation Services (AD FS) to access Azure directly without the need for a third-party IAM product or the need to build certificate authentication for the cloud.

Privileged access/high-security applications

New and varied threat vectors put privileged users like key government officials, and security, network and database admins at great risk. The majority of security breaches involve misuse of privileged credentials. This creates ready access to sensitive information like defense plans, budgets, strategic planning docs, PII/PHI which can cripple the government.

YubiKeys bridge legacy MFA to modern protocols such as FIDO2 and WebAuthn. The YubiKey's hardware design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied or stolen. This offers the highest security for authenticating privileged users.

There are certain scenarios where services may choose to require step-up authentication to complete a high-risk action, such as accessing highly classified systems and documents, as well as highly sensitive administrative actions. The YubiKey can be used as an additional form of validation for high-security applications, to quickly re-verify the user before access is granted or a required action is taken.



RSA SecureID replacement

EO 14028 and OMB M-22-09 have deprecated the use of one-time passcodes, requiring agencies to adopt more secure phishing-resistant authentication. As organizations bridge to this requirement, the first step can be to switch to the Yubico Authenticator as a second factor in an authentication process. The Yubico Authenticator app allows you to store your credentials on a YubiKey and not on your mobile phone, so that your secrets cannot be compromised. The Authenticator App requires a YubiKey 5 Series to generate OTP codes.

Air-gapped networks & SCIFS

Air gap networks are closed off from the outside, making it difficult to authenticate users using data sent over a network. Many air-gapped systems still use username and password or a combination of passwords and a digital identity since the use of a smart card would require additional, expensive readers and would introduce security concerns for the air gap network.

YubiKeys don't need any network connectivity, cellular connection or batteries to work. YubiKeys ensure that air gap networks stay secured against breaches by providing a multi-factor authentication solution that works well in isolated network and mobile restricted environments. With a YubiKey, users can be authenticated without transfer of information across a Cross Domain Solution (CDS).

BYOD
bring your own device



BYOAD
bring your own approved device



AMD
approved mobile device



GFE
government furnished equipment



Mobile devices

The federal government has acknowledged that there are benefits associated with the use of non-GFEs, not the least of which is a reduction in cost, but that such benefits must be weighed against security risks. On August 10, 2022, a DoD memorandum outlined the minimum requirements for the use of non-government owned mobile devices, including the need for authentication with a CAC or DoD-approved authenticator such as the YubiKey.²⁹

Whether BYOAD or GFE, most mobile devices don't support smart card-based authentication. With the YubiKey as a portable root of trust, government workers, contractors and DIB partners can authorize their personal mobile devices for use on government networks and to install government applications, mobile device management applications, or email programs to make these devices trusted. Devices need to be authorized only a single time, with optional support for users to re-authenticate (step-up authentication) to specific government apps and services.

As the number of devices per employee increases, having a single portable external authenticator that can work across all computing devices helps make these transitions seamless.

Government teleworkers

Like other industries, federal agencies now face the reality of long-term hybrid and remote work. As temporary memorandums are replaced with security frameworks and regulations that acknowledge the need to support and secure a remote workforce to federal systems, federal agencies need to re-evaluate any temporary solutions put in place and look for long-term solutions to future-proof access and authentication needs.

The YubiKey works with leading IAM and IdP solution providers to enable remote and hybrid employees to work without the hassle or security risks associated with legacy authentication solutions such as SMS and mobile authenticators. Further, in cases where VPN and Identity-Aware Proxies (IAP) solutions are still in use (as agencies shift to Zero Trust), the YubiKey provides a strong hardware-backed AAL3 token to help support what's in place today as a bridge to more modern architecture.

In cases where remote and hybrid workers are sent GFE devices, the YubiKey can be used as a portable root of trust to ensure the device hasn't been compromised on route.





Supply chain security

The Federal Government relies heavily on software developed internally and from technology vendors. Most software today supports smart cards for authentication or is tied into Active directory, but Zero Trust has now mandated that all software, including cloud, support authentication on their own. As vendors hurry to modify their offering to support zero trust and pass their CMMC audit, the YubiKey offers a bridge solution that can support both smart card and more modern FIDO2/WebAuthn standards.

Further, EO 14028 specifically calls out the lack of transparency and adequate controls to prevent tampering by malicious actors—gaps in the software chain of custody which have been exploited by recent attacks. To improve the verification of the integrity of the software, the YubiKey can be used to help ensure code and commits are Cryptographically signed. Learn more in [Protecting the supply chain with highest-assurance security](#).

“ Meeting this requirement for the general public will mean providing support for Web Authentication-based approaches, such as security keys.”

—OMB M-22-09³¹

Citizen-facing digital services

OMB M-22-09 tasked agencies that provide public-facing services to provide citizens with “tools they can use to protect themselves,” offering more options for authentication within one year.³⁰ Where such agency systems support MFA, they must give users the option to use phishing-resistant MFA, often through the purchase of services from login.gov or building a custom WebAuthn front-end with Azure AD.

Authentication for legacy systems

Most government agencies use a variety of systems, platforms and devices, and not all of these support newer authentication standards such as FIDO and WebAuthn. YubiKeys are appropriate as they support multiple protocols such as smart card (PIV/CAC), FIDO U2F, FIDO2/WebAuthn, OpenPGP, and OTP. The YubiKey’s multi-protocol functionality also helps address a wider range of security needs such as for computer login and remote access, digital signatures for code signing, key escrow for email encryption, or privilege access for older operating environments.

Authentication backup

Regardless of how users are authenticating to their accounts, it is always a best practice to have a backup method in case the primary method of authentication is lost, stolen, broken, or inaccessible. The YubiKey is an affordable, simple option that government workers can carry on their keychain, tuck into a wallet, or store in a safe place for convenient access at any time.



Yubico offers simple procurement and distribution at scale

Yubico offers YubiEnterprise Services, consisting of YubiEnterprise Subscription and YubiEnterprise Delivery, to help simplify procurement and distribution of YubiKeys for employees at scale across various locations.



**YubiEnterprise
Subscription**



**YubiEnterprise
Delivery**

With **YubiEnterprise Subscription**, agencies receive a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, built-in replacements for employee churn, lost or destroyed keys, upgrades to the latest offerings, customer support and more.

With **YubiEnterprise Delivery**, agencies experience turnkey authentication with shipping of YubiKeys, tracking, and returns processing of Yubico products handled seamlessly by logistics experts, so organizations can focus on what matters—securing the workforce.

Takeaway

Every agency today faces a pain point around authentication, whether it's risk or use cases where PIV/CAC is not possible or practical. While regulations such as EO 14028 and OMB M-22-09 have put pressure on agencies to deploy phishing resistant authentication, the mandate to adopt modern authentication is both necessary and timely.

As agencies face looming deadlines and a lack of documented guidance, there is a growing need for cost-effective, turnkey solutions to address the needs of today and future-proof against the authentication needs of tomorrow—including those currently under policy review by the DoD.

The YubiKey provides the highest levels of security needed to address modern day attacks with the flexibility to secure even the most complex scenarios, from air-gapped networks to remote work and cloud services—all from a single key. The YubiKey is a bridge solution that can help support today's problems and build toward the secure, phishing-resistant and passwordless future.

Sources

1. Jason Miller, [DoD plans to bring CAC cards to an end](#), (June 15, 2016)
2. DoD, [Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems](#), (August 20, 2018)
3. Russell T. Vought, [M-19-17](#), (May 21, 2019)
4. Margaret M. Weichert, [M-20-19](#), (March 22, 2020)
5. Homeland Security, [Homeland Security Presidential Directive 12](#), (January 27, 2022)
6. White House, [Moving the U.S. Government Toward Zero Trust Cybersecurity Principles](#), (January 26, 2022)
7. GSA, [Identity Lifecycle Management Playbook version 1.0](#), (June 2022)
8. Verizon, [2022 Data Breach Investigations Report](#), (Accessed August 22, 2022)
9. Stephanie Kelly and Jessica Resnick-ault, [One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators](#)
10. Isabella Jibilian & Katie Canales, [The US is readying sanctions against Russia over the SolarWinds cyber attack](#), (April 15, 2021)
11. Dan Goodin, [A fifth of passwords used by federal agency cracked in security audit](#), (January 10, 2023)
12. White House, [FY2022 budget](#), (Accessed June 1, 2021)
13. The White House, [Executive order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
14. Shalanda D. Young, Office of Management and Budget, [M-22-09](#), (January 26, 2022)
15. White House, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#), (January 19, 2022)
16. NIST, [Digital Identity Guidelines SP 800-63-4](#), (December 2022)
17. GSA, [Identity Lifecycle Management Playbook version 1.0](#), (June 2022)
18. GSA, [Identity Lifecycle Management Playbook version 1.0](#), (June 2022)
19. NIST, [Pre-Draft Call for Comments: Digital Identity Guidelines](#), (June 2020)
20. NIST, [NIST Draft SP 800-63-4](#), (December 2022)
21. CISA, US Digital Service, FedRAMP, [Cloud Security Technical Reference Architecture v 2.0](#), (June 2022)
22. OUSD(A&S), [CMMC Model and Assessment Guides](#), (December 10, 2020)
23. DoD, [Strategic Direction for Cybersecurity Maturity Model Certification \(CMMC\) Program](#), (November 4, 2021)
24. Kim Koster, [NIST 800-171 and CMMC Compliance for Government Contractors](#), (January 31, 2020)
Jerome Becquart, [Ready for CMMC? Here's how you can get there](#), (December 30)
25. DoD Office of the CIO (OCIO), [Memo](#), (August 20, 2018)
26. NIST, [FIPS 201-2](#), (January 2022)
27. GSA, [Identity Lifecycle Management Playbook version 1.0](#), (June 2022)
28. GSA, [Identity Lifecycle Management Playbook version 1.0](#), (June 2022)
29. DoD, [Use of Non-Government Owned Mobile Devices](#), (August 10, 2022)
30. Shalanda D. Young, Office of Management and Budget, [M-22-09](#), (January 26, 2022)
31. Shalanda D. Young, Office of Management and Budget, [M-22-09](#), (January 26, 2022)



About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.